

# SECURE ENDPOINT RELEASE NOTES

Version 5.4

18 March 2024

Secure Endpoint Windows Connector 8.2.4.30130

## Bugfixes/Enhancements

- Resolved Exploit Prevention engine compatibility issue of ntdll unhooking mechanism.

13 March 2024

Secure Endpoint Console 5.4.20240313

## Bugfixes/Enhancements

- Renamed console event types:
  - Threat Detected renamed to File Detection.
  - Threat Detection renamed to Behavioral Threat Detection.

28 February 2024

28 February 2024

## Secure Endpoint Console 5.4.20240228

### Bugfixes/Enhancements

- Minor bugfixes and performance improvements.

14 February 2024

## Secure Endpoint Console 5.4.20240214

### New

- Enabled new UI for device trajectory and inbox pages.

12 February 2024

## Secure Endpoint Windows Connector 8.2.3.30119

### New

- The Behavioral Protection engine can detect and stop threats associated with named pipe creation and connections to named pipes.

### Bugfixes/Enhancements

- Improved clean-up interval and inter-process communication to fix a memory leak in Windows connector 8.2.1 where available RAM would be completely consumed. (CSCwi78497)
- Improved efficacy of the Behavioral Protection engine.
- Exploit Prevention engine bug fixes and enhancements.
- Mitigation for the connector service start failure on servers after Windows updates. (CSCvz56761)
- Fixed a bug where device control rules failed to be updated. (CSCwi37615)
- Fixed an issue where the Secure Client user interface would not launch.
- Fixed an issue that prevented recovery from Cisco Security Connector monitoring service (CCMS) upgrade failures.
- Fixed a ClamAV false positive.
- Fixed an issue that caused Behavioral Protection signature set updates to fail on the first attempt.
- Improved Behavioral Protection logging.
- Cleaned up erroneous integrity check log lines created during install.
- Curl updated to 8.4.0 to fix vulnerabilities.

31 January 2024

- Addressed crashes resulting from invalid event tracing for Windows (ETW) events. (CSCwh85846)
- Fixed a vulnerability in the OLE2 file format parser of ClamAV that could allow an unauthenticated remote attacker to cause a denial of service condition on an affected device as described in CVE-2024-20290. (CSCwh67583)

31 January 2024

## Secure Endpoint Console 5.4.20240131

### Bugfixes/Enhancements

- The [login session duration](#) for a user can now be extended from 30 minutes to 3 hours.
- New Linux connector policies now default to Linux-specific [ClamAV](#) definitions that require less resources by omitting definitions for Windows and Mac systems.
- The Linux [File and Process Scan](#) and Mac [File and Process Scan](#) has been expanded to include 250MB and 500MB in the list of file size options for Maximum Scan File Size and Maximum Archive Scan File Size.

24 January 2024

## Secure Endpoint Linux Connector 1.24.0

### New

- Added support for Amazon Linux 2023 (x86 and ARM).
- Added support for ARM versions of:
  - Amazon Linux 2 (5.x kernels only).
  - Ubuntu 20.04.
  - Ubuntu 22.04.
  - Debian 12.
  - Enterprise Linux 9 including RHEL 9, Alma 9, Rocky 9, and Oracle Linux 9.
- Added support up to mainline kernel version 6.5.
- Added a [connectivity test tool](#) to ampcli.

### Bugfixes/Enhancements

- The ampcli defupdate command now updates both clamav virus definitions and behavioral protection signatures.
- Fixed a bug where invalid scan type and initiator events were being sent to the console.
- Fixed a bug where connector metric data was not being collected properly.

17 January 2024

17 January 2024

## Secure Endpoint Console 5.4.20240117

### Bugfixes/Enhancements

- New online help style with improved search capability.
- Some cloud indications of compromise are available in the Behavioral Protection engine to allow protection actions as well as detections. The new detections are:
  - Compromised plugin.
  - Internet Explorer launched Cscript.
  - Rundll32 launched an encoded Powershell.
  - Spawns a shell.

16 January 2024

## Secure Endpoint iOS Connector 1.6.9

### Bugfixes/Enhancements

- Replaced deprecated crash reporting library.

## Archived release notes

Previous years release notes can be found at the following links:

- [2023 release notes](#)
- [2022 release notes](#)
- [2021 release notes](#)
- [2020 release notes](#)
- [2019 release notes](#)
- [2018 release notes](#)
- [2017 release notes](#)
- [2016 release notes](#)
- [2015 release notes](#)
- [2014 release notes](#)
- [2013 release notes](#)